Australian Government
Department of Education, Employment and Workplace Relations

CPPSEC5005A Implement security risk management plan

Release: 1

INDUSTRY SKILLS COUNCILS
Creating Australia's Future

CPPSEC5005A Implement security risk management plan

Modification History

Not Applicable

Unit Descriptor

Unit descriptor

This unit of competency specifies the outcomes required to facilitate implementation of a security risk management plan. It requires the ability to allocate roles and responsibilities, coordinate and monitor implementation procedures, and evaluate the effectiveness of treatment options.

This unit may form part of the licensing requirements for persons engaged in risk assessment operations in those states and territories where these are regulated activities.

Application of the Unit

Application of the unit

This unit of competency has wide application in a range of managerial roles in the security industry. Work is performed under minimal supervision and competency requires a high level of judgement and decision-making. The knowledge and skills described in this unit are to be applied within relevant legislative and organisational guidelines.

Licensing/Regulatory Information

Refer to Unit Descriptor

Pre-Requisites

Not Applicable

Employability Skills Information

Employability skills	This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Elements describe the essential outcomes of a unit of competency.	Performance criteria describe the required performance needed to demonstrate achievement of the element. Where ***bold italicised*** text is used, further information is detailed in the required skills and knowledge section and/or the range statement. Assessment of performance is to be consistent with the evidence guide.

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
1 **Organise functions and tasks**.	1.1 Applicable provisions of ***legislative*** and ***organisational requirements***, and ***relevant standards*** for ***risk*** assessment activities are identified and complied with. 1.2 ***Roles and responsibilities*** associated with the implementation of the security risk management plan are clearly defined and articulated to ***relevant persons***. 1.3 ***Activities*** and targets are linked to achievement of milestones and outcomes in project action plans. 1.4 ***Resources***, ***equipment and materials*** to assist plan implementation are suitable to project purposes and available within specified timelines. 1.5 Information related to the implementation of the plan is accurately and promptly distributed using established communication channels. 1.6 Confidentiality requirements are confirmed and maintained in accordance with client and organisational requirements.
2 **Monitor risk context**.	2.1 Emerging risks or threats to assets are monitored and assessed to maintain ongoing suitability of implemented security risk ***treatment options***. 2.2 Changes to operating environment are monitored and corrective measures determined and incorporated into the plan as required. 2.3 ***Targets and outcomes*** are regularly reviewed and evaluated to ensure achievement of ***project aims*** based on relevant standards. 2.4 Existence and occurrence of risks are accurately and comprehensively documented providing an assessment of the type, nature and cause. 2.5 Application of contingencies and corrective measures are accurately documented.
3 **Review effectiveness of treatment options**.	3.1 Long and short-term options are costed to ensure an accurate estimate of resources is allocated to support the plans. 3.2 Discrepancies between treatment options and risk incidence are monitored and addressed through appropriate modifications to plans. 3.3 Stages of implementation are identified and resources and options are coordinated to ensure access and availability. 3.4 Corrective measures are developed, tested and incorporated into the risk management plan.

ELEMENT	PERFORMANCE CRITERIA
	3.5 Feedback on effectiveness of treatment options is sought and provided to relevant personnel.

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

This section describes the skills and knowledge and their level required for this unit.

Required skills

- allocate work tasks and functions
- coaching and mentoring to provide support to colleagues
- collate and analyse numerical data
- communicate in a clear and concise manner
- delegate roles and responsibilities
- determine suitability of treatment option against security risk
- determine type and nature of security risks and threats
- manage projects
- monitor implementation procedures
- monitor risk context and identify emerging risks or threats to assets
- prepare and present verbal and written reports
- prioritise tasks and organise schedules
- prioritise treatment options in terms of degree of security risk
- provide written communication to a standard required for compiling reports and summarising information
- relate to persons of different social and cultural backgrounds and varying physical and mental abilities
- research and analyse data and information
- summarise information
- use a variety of problem-solving techniques
- use business equipment and technology.

Required knowledge

- availability and capability of project management software
- concept of integrated security measures including physical security; information technology security, and security of personnel and information
- current security systems and technologies and available expertise
- operating environment and business operations
- preparation of documentation procedures
- principles of effective communication

REQUIRED SKILLS AND KNOWLEDGE

- principles of AS/NZS 4360: 2004 Risk management and related guidelines
- privacy and confidentiality requirements
- process of security risk management
- relevant legislation and regulations including licensing requirements
- risk assessment techniques and processes
- sources of supply of security equipment and systems
- types of treatment options appropriate to the range of security risks and threats applicable to premises and businesses.

Evidence Guide

EVIDENCE GUIDE

The evidence guide provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge, range statement and the Assessment Guidelines for the Training Package.

Critical aspects for assessment and evidence required to demonstrate competency in this unit

A person who demonstrates competency in this unit must be able to provide evidence of:

- monitoring emerging risks to ensure ongoing suitability of risk management plan based on principles of AS/NZS 4360: 2004
- efficient allocation of resources to support risk management plan
- effectively communicating designated roles, responsibilities and work schedules to security personnel
- preparing documentation and guidelines with a clear explanation of the incidence, nature and causes of risks and appropriate contingency arrangements
- systematically reviewing the effectiveness of treatment options and making appropriate modifications as required to address any discrepancies between treatment options and risk incidence.

Context of and specific resources for assessment

Context of assessment includes:

- a setting in the workplace or environment that simulates the conditions of performance described in the elements, performance criteria and range statement.

Resource implications for assessment include:

- access to a registered provider of assessment services
- access to a suitable venue and equipment
- access to plain English version of relevant statutes and

procedures

- assessment instruments including personal planner and assessment record book
- work schedules, organisational policies and duty statements.

Reasonable adjustments must be made to assessment processes where required for people with disabilities. This could include access to modified equipment and other physical resources, and the provision of appropriate assessment support.

Method of assessment

This unit of competency should be assessed using questioning of underpinning knowledge and skills.

Guidance information for assessment

Assessment processes and techniques must be culturally appropriate and suitable to the language, literacy and numeracy capacity of the candidate and the competency being assessed. In all cases where practical assessment is used, it should be combined with targeted questioning to assess the underpinning knowledge.

Oral questioning or written assessment may be used to assess underpinning knowledge. In assessment situations where the candidate is offered a choice between oral questioning and written assessment, questions are to be identical.

Supplementary evidence may be obtained from relevant authenticated correspondence from existing supervisors, team leaders or specialist training staff.

Range Statement

RANGE STATEMENT

The range statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold italicised wording, if used in the performance criteria, is detailed below. Essential operating conditions that may be present with training and assessment (depending on the work situation, needs of the candidate, accessibility of the item, and local industry and regional contexts) may also be included.

Legislative requirements may relate to:

- apprehension and powers of arrest
- Australian standards and quality assurance requirements
- cabling
- counter-terrorism
- crowd control and control of persons under the influence of intoxicating substances
- Force continuum, use of force guidelines

- general 'duty of care' responsibilities
- inspection of people and property, and search and seizure of goods
- licensing or certification requirements
- privacy and confidentiality
- relevant commonwealth, state and territory legislation, codes and national standards for:
    - anti-discrimination
    - cultural and ethnic diversity
    - environmental issues
    - equal employment opportunity
    - industrial relations
    - Occupational Health and Safety (OHS)
- relevant industry codes of practice
- surveillance
- telecommunications
- trespass and the removal of persons
- use of listening and recording devices
- use of restraints and weapons:
    - batons
    - firearms
    - handcuffs
    - spray.

Organisational requirements may relate to:

- access and equity policies, principles and practices
- business and performance plans
- client service standards
- code of conduct, code of ethics
- communication and reporting procedures
- complaint and dispute resolution procedures
- emergency and evacuation procedures
- employer and employee rights and responsibilities
- OHS policies, procedures and programs
- own role, responsibility and authority
- personal and professional development
- privacy and confidentiality of information
- quality assurance and continuous improvement processes and standards
- resource parameters and procedures
- roles, functions and responsibilities of security personnel
- storage and disposal of information.

Relevant standards:

- must include AS/NZS 4360: 2004 Risk management

- may relate to:
  - AS2630-1983 Guide to the selection and application of intruder alarm systems for domestic and business premises
  - HB 167:2006 Security Risk Management
  - HB 436 Risk Management Guidelines - Companion to AS/NZS 4360
  - HB 231:2000 Information security risk management guidelines.

***Risk* relates to**:

- the chance of something happening that will have an impact on objectives.

Security risks may relate to:

- biological hazards
- chemical spills
- client contact
- electrical faults
- explosives
- financial viability
- injury to personnel
- noise, light, heat, smoke
- persons carrying weapons
- persons causing a public nuisance
- persons demonstrating suspicious behaviour
- persons suffering from emotional or physical distress
- persons under the influence of intoxicating substances
- persons with criminal intent
- persons, vehicles and equipment in unsuitable locations
- property or people
- security systems
- suspicious packages or substances
- systems or process failures
- terrorism
- violence or physical threats.

Roles and responsibilities may relate to:

- administrative support
- backup operational role
- decision-making
- frontline role
- team leadership
- team membership.

Relevant persons may include:

- client
- colleagues
- human resources personnel
- management

- security personnel.

Activities may include:

- advising
- field work
- monitoring
- organising
- report preparation
- reporting.

Resources, equipment and materials may relate to:

- consumables
- equipment
- funding
- personnel
- time
- vehicles.

***Treatment options* may relate to**:

- controlled interruptions to normal operations
- exercises
- information collation and analysis
- simulations
- surveillance
- verification requirements.

***Targets and outcomes* may relate to**:

- client support times
- effective security risk management
- incident reports
- level of feedback from clients
- number of new sales
- police liaison
- response times.

***Project aims* may relate to**:

- key outcomes
- milestones
- personnel involvement
- resources
- tasks
- timelines.

Unit Sector(s)

Unit sector Security

Competency field

Competency field	Security and risk management